



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/894,918	06/29/2001	Brian Jacoby	06975-203001/Security 14	5947

26171 7590 09/20/2007
FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER

BOUTAH, ALINA A

ART UNIT	PAPER NUMBER
----------	--------------

2143

MAIL DATE	DELIVERY MODE
-----------	---------------

09/20/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

MAILED

SEP 19 2007

Technology Center 2100

Application Number: 09/894,918
Filing Date: June 29, 2001
Appellant(s): JACOBY ET AL.

W. Karl Renner
Reg. No. 41,265
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed June 20, 2007 appealing from the Office action mailed August 9, 2006.

Art Unit: 2143

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,738,814	Cox et al.	5-2004
6,662,230	Eichstaedt et al.	12-2003
6,654,373	Maher, III et al.	6,654,373
6,337,899	Alcendor	1-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 3-7, 11-12, 16-17, 19-20, 22-26, 28, 30-31, 35-36, 38-39, 41-45, 47, 49-50, 54-55, 57-62, 64 and 68-70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cox (U.S. Patent No. 6,738,814; hereinafter Cox) in view of Eichstaedt et al. (U.S. Patent No. 6,62,230; hereinafter Eichstaedt) in further view of Maher, III et al. (U.S. Patent No. 6,654,373; hereinafter Maher), in further view of Alcendor et al. (U.S. Patent No. 6,337,899; hereinafter Alcendor).

In considering claims 1, 4-5, 19-20, 22-23, 38-39 and 41-42, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses a method for securing an accessible computer system, the method comprising:

Art Unit: 2143

receiving more than one data packet at a network device (see Cox: col. 3, lines 26-29) each includes a payload portion and an attribute portion (see Cox: fig. 2 step 20 and col. 3, lines 30-33), received packets are analyzed; packets include a payload portion and an attribute portion and are communicated between at least one access requestor (see Cox: fig. 1, means 16, access requestor or attacker) and at least one access provider through the network device (see Cox: fig. 1 means 12, access provider); monitoring at the network device at least the payload portion of the data packet received by scanning the payload portion for at least one predetermined pattern (see Cox: col. 3, lines 41-45); While Cox discloses analyzing incoming packets against known patterns and denying access to the access provider by the access requestor when there is a match of the known pattern, Cox does not disclose the step of counting the number of data packets that include the predetermined pattern and denying access when that number exceeds a configurable threshold.

Nonetheless, denying access to client computers of data object access through a server computer when a predefined minimum value is exceeded is well known as evidenced by Eichstaedt. In similar art Eichstaedt discloses a method for automatically limiting access of a client computer to data objects accessed through a server computer wherein when a server receives a data request (packet) from a client machine over the network, the request values of the received request having a client identifier (pattern) matching a logged entry are calculated and compared to a predefined maximum request values. If the request values exceed a corresponding predefined maximum request value, the request is refused or denied (see Eichstaedt col. 6, lines 46-61).

Art Unit: 2143

It would have been obvious to a person having ordinary skill in the art to modify the system for blocking denial of service attacks to include the step of counting a number of data packets including a predetermined pattern in addition to matching the predetermined pattern and denying access when that number exceeds a configurable threshold in order to decrease or deny abusive traffic (i.e. denial of service attacks) thereby preventing server or website shut downs, flooding, and overloading. Attacks can cause websites to temporarily cease operation and interrupt access by legitimate consumers, it would thus be advantageous to incorporate such a system to avoid such a costly, in both time and money; non-operation period. Therefore the claimed limitations would have been obvious modifications.

Cox further discloses denying access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed the threshold number (see Cox col. 3, lines 41-54). While Cox discloses analyzing the incoming packet against known patterns, Cox does not explicitly disclose that the monitoring includes scanning at least the payload portion of the data packet for at least one predetermined pattern. Nonetheless, scanning the packet's payload and matching it against known patterns or strings is well known as evidenced by Maher. In similar art, Maher discloses a payload analyzer that scans the contents of data packet's payload and attempts to match the payload contents against a database of known strings (col. 2, lines 64-66).

According to Maher, the ability to look beyond the header information, while still in the fast-path and into the packet contents; would allow a network device to identify the nature of the information carried in the packet, thereby allowing much more detailed packet classification. The knowledge of the content would also allow specific contents to be identified and scanned to

Art Unit: 2143

provide security such as virus detection, denial of service prevention, etc. It would have been obvious for a person having ordinary skill in the art, to modify the system as taught by Cox to include the step of scanning the entire packet including the payload in order to maintain an awareness of content over an entire traffic flow, and identify and filter out security problems such as email worms, viruses, denial of service attacks, and illegal hacking.

Cox also fails to explicitly teach monitoring the payload portion of the data packets directed from at least one of the access providers to at least one of the access requestors, and denying subsequent when the number of the data packets received from the access provider to the access requestor exceeds a configurable threshold number. Nonetheless, this feature is being taught by Alcendor, which discloses limiting a number of login retries in a server, and rejecting the login attempt based on the number of login retries from the server to the client (see col. 7, lines 27-33).

At the time the invention was made, one of ordinary skill in the art would have been motivated to monitor and limit data packets directed from the access provider to the access requestor in order to limit the amount of access in the system, therefore enhancing its security.

In considering claims 3, 22, and 41, the combined system of Cox, Eichstaedt, Maher and Alcendor that: monitoring the data packets includes scanning the payload portion while handling the data packets with a switch (See Maher, col. 11, lines 3-17).

Art Unit: 2143

In considering claims 6, 25, and 44, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses that at least one data packet is distinguished based on an Internet address associated with the packet (See Eichstaedt col. 6, lines 46-48).

In considering claims 7, 26, and 45, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses that receiving the data packet includes receiving more than one data packet; and monitoring the data packet includes monitoring all of the data packets received (See Maher col. 7, lines 10-19).

In considering claims 28, and 47, the combined system of Cox, Eichstaedt, and Maher and Alcendor discloses that the data packets are monitored when communicated from the client to the host or from host to the client (See Maher col. 3, lines 39-45).

In considering claims 11, 30, and 49, the combined system of Cox, Eichstaedt, and Maher and Alcendor discloses that the predetermined pattern includes a login failure message communicated from the access requestor to the access provider (See Maher col. 7, lines 15-17).

In considering claims 12, 31, and 50, although the combined system of Cox, Eichstaedt, Maher and Alcendor discloses the system substantially as claimed, it does not specifically disclose that the data packets include a token-based protocol packet, a TCP packet or a PPP packet. Examiner takes official notice that the aforementioned packets are well known packets of well-known Internet protocols such as TCP and PPP. A person having ordinary skill

Art Unit: 2143

in the art would have readily recognized the uses and advantages of including different types of protocols and their respective packets in order to comply with multiple standards thus making the system more extensible. Therefore the claimed limitation would have been an obvious modification.

In considering claims 16, 35, and 54, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses that denying communication of subsequent data packets includes affecting bandwidth for communications between the access requestor and the access provider (See Maher col. 7, lines 56-67 through col. 8, lines 1-6).

In considering claims 17, 36, and 55, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses that denying access includes rerouting the access requestor (See Maher col. 3, lines 25- 38).

In considering claims 19, 38, 57, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses that receiving the data packet includes receiving more than one data packet; and denying subsequent data packets from the requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number during a configurable period of time (See Cox. col. 3, lines 11-29 and col. 4, lines 16-40).

In considering claim 58, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses the method as in claim 1 wherein denying subsequent access by the access requestor to

Art Unit: 2143

the access provider further comprises denying subsequent access from a group of access requestors to the access provider when a number of payload portions within the data packets that are received from the access provider by at least one access requestor which is a group member, include the predetermined pattern exceed a configurable threshold number (See Cox. col. 3, lines 11-29 and col. 4, lines 16-40).

In considering claim 59, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses the method of claim 1 further comprises determining whether the access requestor is on a permitted access list that is associated with the access requestors, allowing subsequent access from the access requestor to the access provider conditioned on whether or not the access requestor is determined to be included in the permitted access list (See Cox. col. 3, lines 11-29 and col. 4, lines 16-40).

In considering claim 60, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses the method of claim 59 wherein determining whether the access requestor is included in the permitted access list further comprises determining whether the IP address of the access requestor is included in the permitted access list (see Eichstaedt col. 6, lines 46-61).

In considering claim 61, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses the method of claim 1 wherein subsequent access by the access requestor to the access provider is denied for a pre-determined and limited period of time (see Alcendor, col. 7, lines 27-33).

Art Unit: 2143

In considering claim 62, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses the method of claim 61 wherein denial of subsequent access by the access provider starts a new pre-determined and limited time period upon detecting an access request from the access requestor during the elapsing of the predetermined and limited period of time (see Alcendor, col. 7, lines 27-33).

In considering claim 64, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses the method of claim 1, wherein denying subsequent access by the access requestor is performed in response to a command received from the access provider, irrespective of the inspection of data packets received from the access provider (see Alcendor, col. 7, lines 27-33).

In considering claim 67, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses the method of claim 11 wherein the predetermined pattern further includes a login request message (see Alcendor, col. 7, lines 27-33).

In considering claim 68, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses the method of claim 11 wherein the login failure message includes a signature located at a specific offset from an end of the data packet communicated from the access provider of the access requestor (see Alcendor, col. 7, lines 27-33).

Art Unit: 2143

In considering claim 69, the combined system of Cox, Eichstaedt, Maher and Alcendor discloses the method of claim 11 wherein login failure message includes login failure reasons (see Alcendor, col. 7, lines 27-33).

In considering claim 70, the combined method of Cox, Eichstaedt, Maher and Alcendor discloses the method of claim 1 wherein the network device is physically independent process from the access providers (See Cox: figure 1).

In considering claim 71, the combined method of Cox, Eichstaedt, Maher and Alcendor discloses the method of claim 1 wherein the network device is a switch (see Cox, figure 1).

In considering claim 72, the combined method of Cox, Eichstaedt, Maher and Alcendor discloses the method of claim 1 wherein the access provider is a device configurable to make a determination of whether access is permitted (see Eichstaedt col. 6, lines 46-61).

In considering claim 73, the combined method of Cox, Eichstaedt, Maher and Alcendor discloses the method of claim 72 wherein the access provider is the field arbitrator of whether access is provided (see Eichstaedt col. 6, lines 46-61).

(10) Response to Argument

Appellant argues that none of the cited art of record suggest the feature of denying subsequent data packets from access requestors based on the result of monitoring the payload portion of the data packets directed from access providers.

The PTO respectfully submits that this feature is taught by Cox, Eichstaedt, Maher and Alcendor combined. Specifically, Cox teaches monitoring, at the network device, at least the payload portion of the data packet received by scanning the payload portion for at least one predetermined pattern (see Cox: col. 3, lines 41-45 – “The routing device can then match the analyzed packets against the patterns to determine whether or not some type of attack is being made. If an attack is identified, the routing device can identify the source of that packet as malicious and treat the source accordingly.”). Cox also discloses denying subsequent data packets from access requestors based on the result of monitoring the payload portion of the data packets (see Cox: col. 3, lines 46-54 – “the routing device can implement methods for blocking denial of service attacks and address spoofing attacks as shown, for example, in Figs. 3 and 4.”).

In similar art Eichstaedt discloses a method for automatically limiting access of a client computer (interpreted as “access requestor”) to data objects accessed through a server computer (interpreted as “access provider”) wherein when a server receives a data request (packet) from a client machine over the network, the request values of the received request having a client identifier (pattern) matching a logged entry are calculated and compared to a predefined maximum request values. If the request values exceed a corresponding predefined maximum request value, the request is refused or denied (see Eichstaedt col. 6, lines 46-61).

In another analogous art, Alcendor discloses a user (interpreted as “access requestor”) accessing a desired service, such as ISPs and other providers (interpreted as “access provider”) (see Alcendor, col. 7, lines 3-5). Once the user is connected to the desired service, the user is authenticated into desired service by known techniques (col. 7, lines 10-20). If the user’s

Art Unit: 2143

authentication fails, the user has a predetermined number of retries (col. 7, lines 27-33). As evidenced by the cited art, there is suggestion that the access is monitored from the access provider itself.

In response to Appellant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

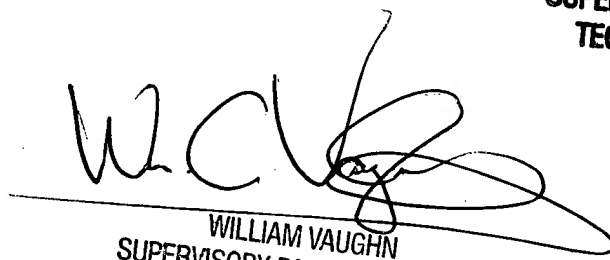
For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

ANB

ANB

Conferees:


WILLIAM VAUGHN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100